

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339273
(43)Date of publication of application : 08.12.2000

(51)Int.Cl. G06F 15/00

(21)Application number : 11-152382

(71)Applicant : NEC CORP
NEC SOFTWARE TOHOKU LTD

(22)Date of filing : 31.05.1999

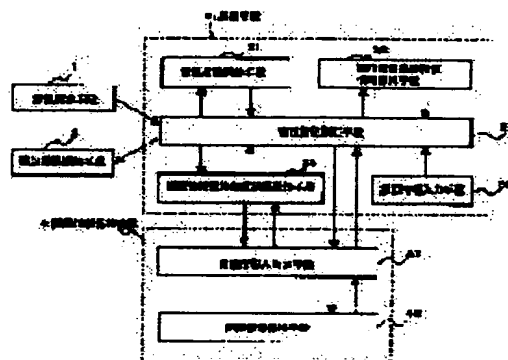
(72)Inventor : KOMATSU FUMIKO
HIDANO MORIMITSU

(54) INFORMATION PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a device which simplifies an authentication procedure at the time of using an application and, at the same time, enables authentication information to be used in common by plural applications.

SOLUTION: This device is an authentication system which enables authentication information for a user to be used in common among plural applications for performing authentication when the user accesses the information. When the system is fitted with an authentication information holding device 4 which is freely attachable/detachable and stores the authentication information, in active state and authentication is already performed, an authentication procedure at the time of using the application is not performed but the application is accessed as it is. When the authentication information holding device 4 is removed and is not activated, switch control is performed so that an authentication procedures needed by the application is performed in using the application.



LEGAL STATUS

[Date of request for examination] 21.04.2000

[Date of sending the examiner's decision of rejection] 12.08.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-339273
(P2000-339273A)

(43) 公開日 平成12年12月8日 (2000. 12. 8)

(51) Int.Cl.⁷
G 0 6 F 15/00

識別記号
3 3 0

F I
G 0 6 F 15/00

テーマコード(参考)

3 3 0 G 5 B 0 8 5

審査請求 有 請求項の数 8 O L (全 9 頁)

(21) 出願番号 特願平11-152382

(22) 出願日 平成11年5月31日 (1999. 5. 31)

(71) 出願人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(71) 出願人 000222059

東北日本電気ソフトウェア株式会社
宮城県仙台市青葉区一番町一丁目10番23号

(72) 発明者 小松 文子

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100080816

弁理士 加藤 朝道

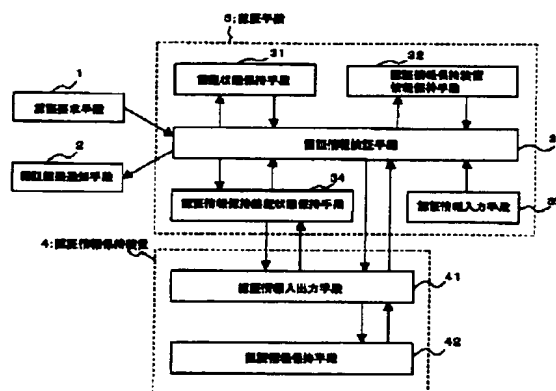
最終頁に続く

(54) 【発明の名称】 情報処理装置

(57) 【要約】

【課題】アプリケーション利用時の認証手順を簡素化するとともに、複数のアプリケーションで認証情報を共用可能とする装置の提供。

【解決手段】ユーザがアクセスする際に認証を行う複数のアプリケーション間で前記ユーザの認証情報を共有可能とする認証システムであって、認証情報を格納する着脱自在な認証情報保持装置が装着されて活性化状態にあり、且つ、認証済みである場合には、アプリケーションの利用時の認証手続は行わず、そのまま前記アプリケーションがアクセスされ、一方、前記認証情報保持装置が外されている等活性化されない時には、アプリケーションを利用する際に前記アプリケーションで必要とされる認証手続を行うように切替制御する。



【特許請求の範囲】

【請求項 1】ユーザがアクセスする際に本人認証を行う複数のアプリケーション間で前記ユーザの認証情報を共有可能とする情報処理装置であって、
認証情報を格納する着脱自在な認証情報保持装置が装着されて活性化状態にあり、且つ、認証済みであることを検出した場合には、アプリケーションの利用時の本人認証手続きは行わず、そのまま前記アプリケーションがアクセスされ、一方、前記認証情報保持装置が活性化できない時には、アプリケーションを利用する際に前記アプリケーションで必要とされる本人認証手続きを行うように切替制御する手段を備えたことを特徴とする情報処理装置。

【請求項 2】前記着脱自在な認証情報保持装置記が、ユーザからの本人認証情報を入力する手段と、認証情報の検証を行なう手段と、認証情報を保持する手段とを含むことを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】認証情報を着脱自在な認証情報保持装置に記憶保持し、

アプリケーション利用の際の本人認証時、認証要求を受けた際に、前記認証情報保持装置が装着されて活性化状態とされ、且つ記憶手段に保持された、認証済みであるか否かを示す認証状態情報が認証済みであることを示す場合には、認証手順を省略して認証成功を通知するように制御する手段を備え、前記アプリケーションは認証成功の場合、本人認証手続きを省略し、
前記認証情報保持装置が活性化状態にない場合、もしくは活性化できない場合、前記認証状態情報をリセットし、前記アプリケーションで必要とされる本人認証手続きを行なうように制御する手段を備えたことを特徴とする情報処理装置。

【請求項 4】アプリケーション利用の際の本人認証時、前記認証情報保持装置が装着状態にあり、前記認証状態フラグが認証済みでないことを示す場合には、本人認証手続きを実行し、本人であることが認証された場合、前記認証状態情報を認証済みに設定する手段を備えたことを特徴とする請求項 3 記載の情報処理装置。

【請求項 5】前記着脱自在な認証情報保持装置の装置の特性及び状態を取得する手段を備えたことを特徴とする請求項 3 記載の情報処理装置。

【請求項 6】アプリケーションで本人認証手続きが必要とされた場合に前記アプリケーションから起動される認証要求手段と、前記認証要求手段からの認証要求を受け取り、着脱自在な認証情報保持装置の状態情報を取得し、活性化状態であれば、認証状態を取得し、未認証状態であれば、前記認証保持装置が保持しているユーザ本人の認証情報と、入力手段から入力された認証情報との照合を行い、ユーザ本人であることを認証がなされた場合、認証状態を認証済みに設定し、認証済み状態であれば、認証処理を省略し認証成功を認証結果通知手段に出

力する認証手段を備え、前記認証成功が出力された場合、前記アプリケーションは本人認証手続きを省略する、ことを特徴とする情報処理装置。

【請求項 7】前記認証情報保持装置が、記憶媒体もしくは IC カードよりなることを特徴とする請求項 3 乃至 6 のいずれかに記載の情報処理装置。

【請求項 8】前記アプリケーションは、前記認証要求手段と前記認証結果通知手段を介して前記認証手段と交信し、前記認証情報保持装置の制御は前記認証手段で行うことを特徴とする請求項 6 記載の情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置に関し、特に、情報処理装置で稼働するアプリケーションを利用する際の認証を行うシステムに関する。

【0002】

【従来の技術】コンピュータ等情報処理装置上でアプリケーションを利用する場合、正当な利用者であることの認証を行うため、アプリケーションは、ログイン時、ユーザにユーザ ID 及びパスワードの入力を督促し、入力されたユーザ ID、パスワードが登録されたものと一致する場合、アプリケーションの利用が許可される構成とされている。

【0003】ところで、アプリケーションを利用するたびに認証手順を行うことは、煩雑であることから、ひとたび、本人から入力され照合された認証情報を、ハードディスクやメモリ上に保持し、2 回目以降の本人認証には、該媒体に保持された情報を使用することで、認証回数を削減するようにしたアプリケーションも存在している。

【0004】

【発明が解決しようとする課題】しかしながら、このように認証回数を削減する従来のシステムは、次のような問題点を有している。

【0005】第 1 の問題点は、認証情報の漏洩など、セキュリティの面が十分に考慮されていない、ということである。

【0006】その理由は、将来のシステムは、本人から入力された認証情報を、情報処理装置に固定のハードディスクやメモリ上に保持し、2 回目以降の本人認証には、保持した情報を使用するというものであるためである。また、情報そのものが盗まれなくとも、例えば利用者が席を外している間に第 3 者が利用者になりすまし、不正にアプリケーションを利用することも可能である。

【0007】第 2 の問題点は、情報処理装置で稼働するアプリケーションの数だけ本人認証が発生する、ということである。

【0008】その理由は、アプリケーションによって実装方法が異なるため、アプリケーション間で認証情報を共有することができないためである。

【0009】なおキーデータが電源供給中保持されることをなくすICカードとして、特開平5-250562号公報には、外部からある命令を入力することで、認証情報の照合結果を内部的にクリアする手段を備え、認証情報の照合結果が電源供給中に保持されることがなくなり、途中で介在する不当者による不正アクセスを防止するようにした構成が開示されている。また特開平10-285153号公報等には、利用者が自己のキーファイルを格納したICカードを装着した場合、利用者認証が行われ、キーファイルをメモリに展開し、またICカードが抜かれた場合、メモリからキーファイルを削除し、第三者への漏洩を防ぐ通信システムが開示されているが、これは、仮想専用回線利用時すなわち単一アプリケーション利用時のキーファイルの漏洩を回避するためのものである。

【0010】したがって本発明は、上記問題点を鑑みてなされたものであって、その主たる目的はアプリケーション利用時の認証手順を簡素化するとともに、複数のアプリケーションで認証情報を共用可能とする情報処理装置を提供することにある。

【0011】

【課題を解決するための手段】前記目的を達成する本発明は、ユーザが利用する際に認証を行う複数のアプリケーションの間で認証情報を共有可能とする認証システムであって、着脱自在な記憶媒体に記憶保持した記憶媒体が装着された状態にあり、且つ、認証済みである場合には、アプリケーション利用時に本人認証手順は行わず、そのままアプリケーションが実行され、一方、前記記憶媒体が外されている時は、アプリケーションを利用する際に本人認証を行うように切替制御する手段を備えたものである。

【0012】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、コンピュータの利用者がコンピュータ上で動作するアプリケーションを利用する際に、アプリケーションによる利用者の本人認証を行うにあたり、本人認証を一度行えば、利用者が着脱自在な記憶デバイスをコンピュータから抜き取らない限り、すでに認証済み状態であれば、これ以降の本人認証を省略可能としたものであり、本人認証の操作・手続きを簡略化する。

【0013】本発明の実施の形態について説明する。本発明の実施の形態は、図1を参照すると、認証要求手段(1)からの本人認証要求を認証情報検証手段(33)が受け取り、本人認証情報の検証結果を認証結果通知手段(2)へ引き渡す。

【0014】認証情報検証手段(33)は、認証情報保持装置状態保持手段(34)から認証情報保持装置の状態を取得し、活性化状態であれば、認証状態保持手段

(31)から認証状態情報(フラグ)を取得し、認証状態が未認証状態であれば、認証保持装置(4)が保持し

ている本人認証情報と、認証検証手段(33)が認証情報入力手段(35)によって利用者から入力された認証情報との照合を行い、その結果を、認証結果通知手段(2)へ検証結果を供給する。

【0015】認証情報検証手段(33)は、認証状態保持手段(31)から取得した認証状態が認証済み状態であれば、認証処理を省略し、認証結果通知手段(2)へ認証成功の旨を通知する。

【0016】このようにして、認証状態を判断し、省略可能な認証手順を適宜省略することにより、認証手順を簡略化している。また一度、本人認証を行えば、他のアプリケーションでの本人認証手順を省略することができる。

【0017】

【実施例】上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して説明する。図1は、本発明の一実施例の構成を示す図である。

【0018】図1を参照すると本実施例は、アプリケーションが発行する認証関数(サブルーチン)群などの認証要求手段1と、認証結果を通知する認証結果通知手段2と、本人であるか否かの認証処理を行う認証手段3と、本人認証に必要となるパスワードや認証子(ID)などの本人認証情報を保持するフロッピーディスクや磁気カードなどの認証情報保持装置4と、を備えている。

【0019】認証手段3は、利用者の認証が、未認証状態であるか認証済み状態であるかの情報を保持する認証状態保持手段31と、認証情報保持装置4の特性等の情報を保持する認証情報保持装置情報保持手段32と、利用者と認証情報保持装置4との認証インターフェースを制御する認証情報検証手段33と、認証情報保持装置4が活性化されているか非活性化されているのかに関する状態情報を保持する認証情報保持装置状態保持手段34と、利用者が保持する本人認証情報を入力するための認証情報入力手段35とを含む。

【0020】認証情報保持装置4は、認証情報を入出力するための認証情報入出力手段41と、入力された本人認証情報を保持するための認証情報保持手段42とを含む。

【0021】これらの手段はそれぞれ概略つぎのように動作する。

【0022】認証要求手段1は、情報処理装置で実行されるアプリケーションで利用者の認証が必要となった場合に該アプリケーションから起動され、本人認証を、認証情報検証手段33に要求する。また、認証要求手段1が認証情報検証手段33に対して要求した認証要求の結果は、認証情報検証手段33から認証結果通知手段2に通知される。

【0023】認証手段3の認証状態保持手段31は、認証情報検証手段33によって検証された結果を保持す

る。

【0024】認証手段3の認証情報保持装置情報保持手段32は、認証情報保持装置のハードウェア特性などの情報を保持する。

【0025】認証手段3の認証情報検証手段33は、認証情報保持装置状態保持手段34から認証情報保持装置4の状態を取得し、活性化状態であれば認証状態保持手段31から認証状態を取得し、当該認証状態が未認証状態であれば認証保持装置4が保持している認証情報と、

認証検証手段33が認証情報入力手段35によって利用者から受け取った認証情報との検証を行い、その結果を、認証結果通知手段2へ検証結果を引き渡す。

【0026】認証状態保持手段31から取得した認証状態が認証済み状態であれば以降の処理を省略し、認証結果通知手段2へ検証結果（本人認証成功）を引き渡す。

【0027】但し、認証情報保持装置状態保持手段34から取得した状態が非活性化状態であれば、認証状態保持手段31から取得した状態を無効とし、未認証状態の場合と同様の手順を取る。

【0028】認証手段3の認証情報入力手段35は、認証情報検証手段33に要求された認証保持装置の特性に合った認証インターフェースのもと、利用者が入力した認証情報を認証情報検証手段33へ供給する。

【0029】認証手段3の認証情報保持装置状態保持手段34は、認証情報保持装置4が活性化されているか非活性化状態にあるかの情報を保持する。

【0030】認証情報保持装置4の認証情報入出力手段41は、認証情報保持手段42で保持されている認証情報の入出力を行う。

【0031】図2、及び図3は、本発明の一実施例の動作を説明するためのフローチャートである。図1乃至図3を参照して本発明の一実施例の動作について説明する。

【0032】まず、認証情報検証手段33が認証要求手段1から要求された認証要求を受け付ける（図2のステップA1）。なお、認証要求手段1は、アプリケーションで本人認証を行うときに起動される。

【0033】次に、認証情報保持装置状態保持手段32から認証情報保持装置4の状態を受け取り（図2のステップA2）、使用する認証情報保持装置4が活性化状態

か否かを判断する（図2のステップA3）。

【0034】認証情報保持装置4が非活性化状態であれば、認証状態保持手段31の認証状態を無条件に未認証状態とし、認証情報保持装置4の活性化を試みる（図2のステップA4）。

【0035】認証情報保持装置4の活性化に失敗した場合、認証不可能と判断し、認証失敗を認証結果通知手段2に通知する（図2のステップA12）。

【0036】一方、活性化に成功した場合、認証情報保持装置状態保持手段34の認証情報保持装置状態を活性

化状態とし（図2のステップA5）、認証状態保持手段31から認証状態を取得する（図2のステップA6）。

【0037】図2のステップA3において、認証情報保持装置4が活性化状態であれば、図2のステップA4とステップ5をスキップし、図2のステップA6を実行する。

【0038】取得した認証状態を検証し（図2のステップA7）、未認証状態であれば認証情報検証処理（図2のステップA8）を実行する。

【0039】認証情報検証処理の結果を判断し（図2のステップA9）、検証失敗であれば図2のステップA12を実行し、検証成功であれば、認証状態保持手段31の認証状態を認証済み状態とし（図2のステップA10）、認証成功を認証結果通知手段2に通知する（図2のステップA11）。

【0040】図2のステップA7で認証済み状態であれば、図2のステップA8とステップ9とステップ10をスキップし、図2のステップA11を実行する。

【0041】次に、本人の認証情報の検証処理（図2のステップA8）を説明する。図3は、図2のステップA8の本人の認証情報の検証処理の処理手順を示すフローチャートである。

【0042】まず、認証情報保持装置情報保持手段32から装置情報を取得する（図3のステップB1）。

【0043】本実施例では、認証情報保持装置4がフロッピーディスクや磁気カードなどの認証情報を保持する機能しか持たない装置であるため、認証情報保持装置4から認証情報を取得する（図3のステップB2）。この時、認証情報の取得に失敗したか否かを検証し（図3のステップB3）、失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図3のステップB4）。

【0044】ステップB3の判定で認証情報の取得に成功した場合、認証情報入力手段35から利用者に対して利用者が保持している認証情報を入力させ（図3のステップB5）、図3のステップB2で取得した認証情報と、図3のステップB5で取得した認証情報を比較し、同じであれば検証成功とし、異なれば検証失敗とする（図3のステップB6）。

【0045】次に、本発明の第2の実施例について説明する。図4は、本発明の第2の実施例の構成を示す図である。図4を参照すると、本発明の第2の実施例においては、図1に示した前記実施例と相違して、認証情報検証手段43と認証情報入力手段44が、認証情報保持装置4に含まれている。この認証情報保持装置4は、前記実施例で用いたフロッピーディスクや磁気カードなどのように情報を保持するだけでなく、例えばICカード等のように、不揮発性の記憶手段のほかに制御装置（LSI）を内蔵し、それ自身で認証情報の検証が可能とされ、また利用者からの認証情報を直接入力可能としてい

る。

【0046】図5は、本発明の第2の実施例の処理を説明するための流れ図である。図を参照すると、図3に示したステップB1とからステップB2の間に、この実施例で用いられる認証情報保持装置4の特性によって、新たに2つのフェーズに分岐している。図5で追加された処理ステップについて以下に詳細に説明する。

【0047】まず、認証情報保持装置情報保持手段32から装置情報を取得し（図5のステップB1）、認証情報保持装置4自身に認証情報入力手段44を保持しているか否かを判断する（図5のステップC1）。 10

【0048】認証情報入力手段44を保持している装置であれば、利用者に対して利用者が保持している認証情報を認証情報保持装置4に入力させ（図3のステップC3）、認証情報検証手段43で検証した結果を認証情報検証手段33が受け取る。この時、認証検証結果の取得に失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図5のステップC5）。

【0049】次に、認証情報保持装置4で認証情報入力手段44を保持していなくとも、認証情報保持装置4が認証情報検証手段43を保持していれば（図5のステップC2）、認証手段3の認証情報入力手段35にて利用者から取得した（図5のステップC6）認証情報を、認証情報保持装置4へ入力し（図5のステップC7）、装置内の認証情報検証手段43が、入力された認証情報と装置自身で保持している認証情報との検証を行う。 20

【0050】検証結果を、認証情報検証手段33が受け取る（図5のステップC8）。

【0051】ステップ7で認証情報の入力に失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図5のステップC5）。 30

【0052】

【発明の効果】以上説明したように、本発明によれば、下記記載の効果を奏する。

【0053】本発明の第1の効果は、最初に利用するアプリケーションで本人認証を行えば、その後、他のアプ

リケーションを利用する際に、本人認証を行う必要がなく、複数のアプリケーション間で認証情報を共有可能とし、利用者にとって使いやすいコンピュータ環境を提供することができる、ということである。

【0054】その理由は、本発明においては、同じ認証情報保持装置を本人認証に用いるアプリケーション間では認証状態を共有することができるためである。

【0055】本発明の第2の効果は、アプリケーションの設計において、汎用的な本人認証の機能を保持したアプリケーションを設計することを可能としている、ということである。

【0056】その理由は、本発明においては、アプリケーション自体は、着脱自在の認証情報保持装置の特性を意識する必要がないために、認証情報保持装置の制御から解放される構成としたためである。

【図面の簡単な説明】

【図1】本発明の第1の実施例の構成を示す図である。

【図2】本発明の第1の実施例の処理を説明するための流れ図である。

【図3】本発明の第1の実施例の処理を説明するための流れ図である。

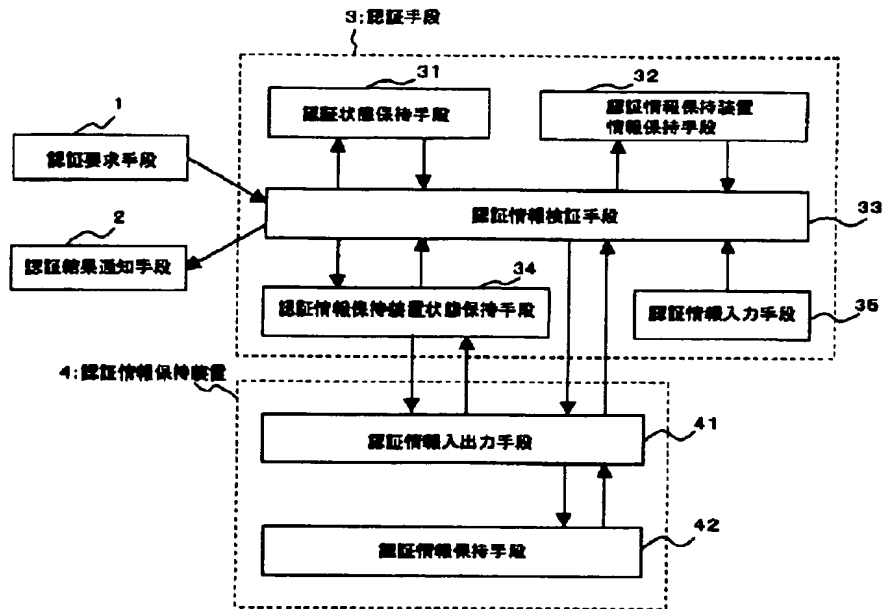
【図4】本発明の第2の実施例の構成を示す図である。

【図5】本発明の第2の実施例の処理を説明するための流れ図である。

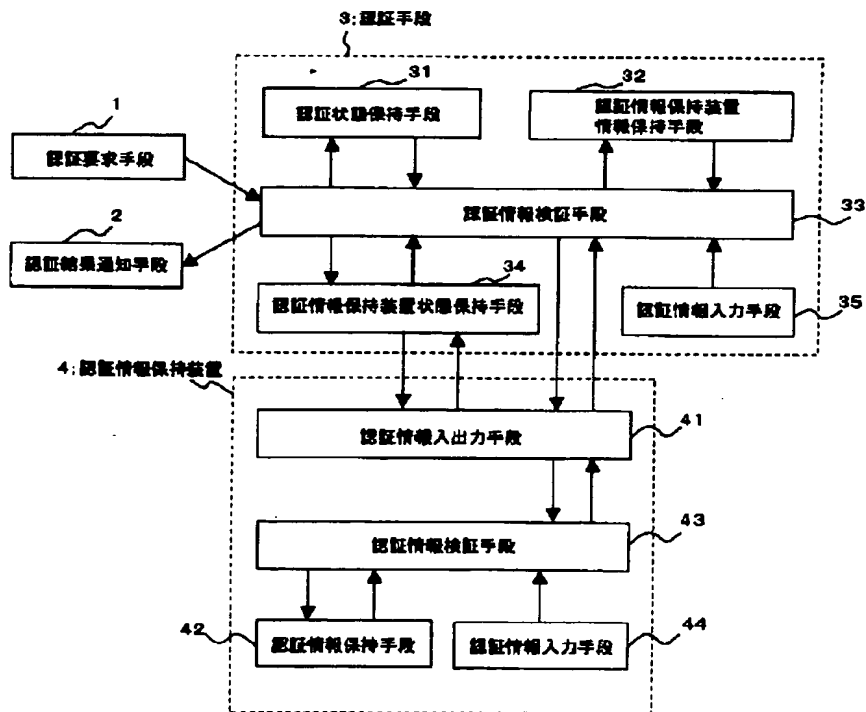
【符号の説明】

- 1 認証要求手段
- 2 認証結果通知手段
- 3 認証手段
- 4 認証情報保持装置
- 31 認証状態保持手段
- 32 認証情報保持装置情報保持手段
- 33 認証情報検証手段
- 34 認証情報保持装置状態保持手段
- 35 認証情報入力手段
- 41 認証情報入出力手段
- 42 認証情報保持手段

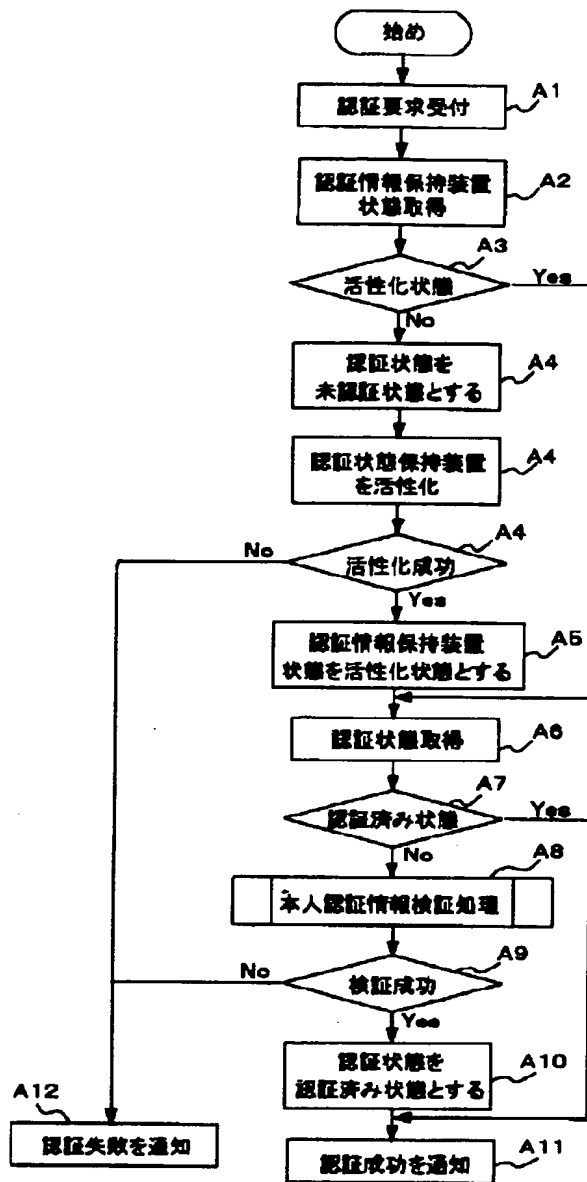
【図1】



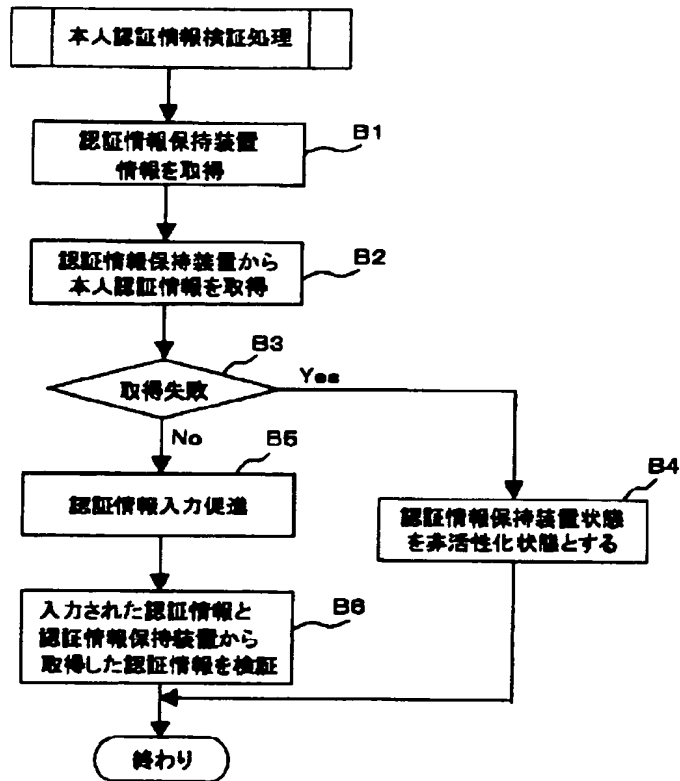
【図4】



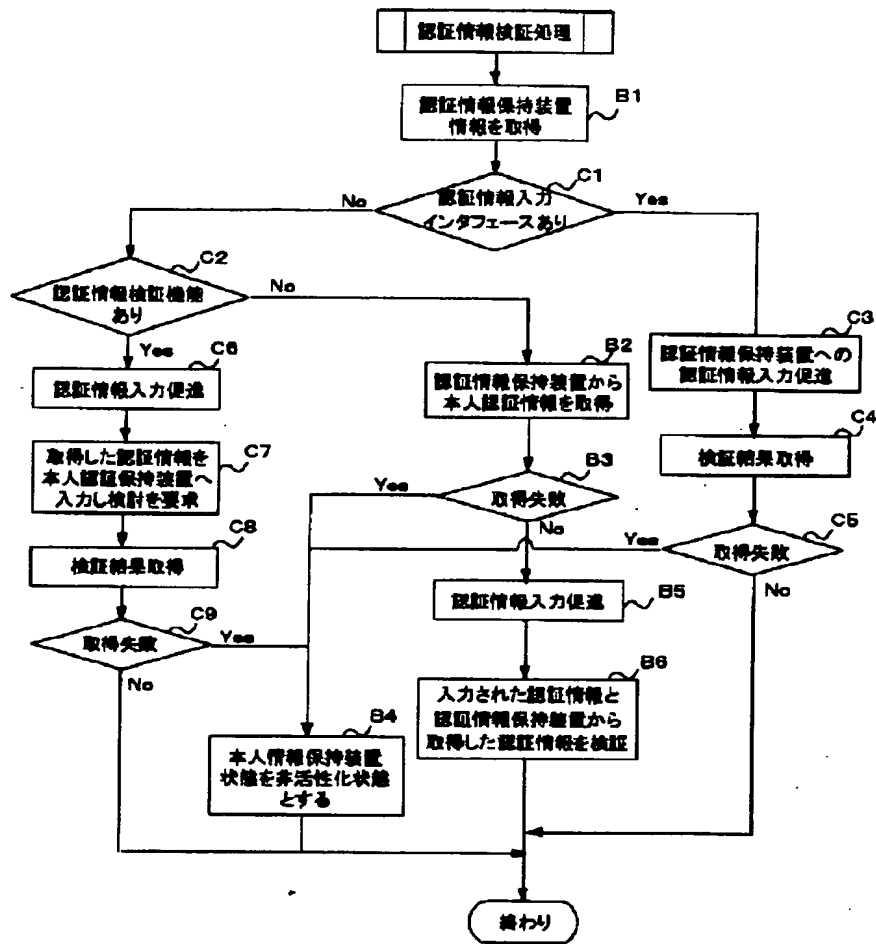
【図2】



【図3】



【図5】



フロントページの続き

(72)発明者 肥田野 守光

宮城県仙台市青葉区一番町1-10-23 東
北日本電気ソフトウェア株式会社内

Fターム(参考) 5B085 AA08 AE06 AE12 AE23

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.